REMARKS/ARGUMENTS

In the final Office action dated May 20, 2005, Claims 1 - 3, 14, 16 - 22, 27, 29 and 30 were rejected under 35 U.S.C. § 102. Claims 4 - 6, 9 - 12 and 24 were rejected under 35 U.S.C. § 103. Claims 7, 8, 13, 15, 23, 26, 28 and 31 were deemed allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Reconsideration and reexamination are hereby requested for Claims 1 - 31 that are pending in this application.

35 U.S.C. §102 Rejections of Claims 1 - 3, 16 - 22 and 27

The Examiner has rejected Claims 1 - 3, 16 - 22, and 27 under 35 U.S.C. §102(e) as being anticipated by Silverbrook et al., U.S. Patent No. 6,334,190 (hereafter "Silverbrook"). Claims 1, 16 and 27 are independent claims.

Claim 1 recites, in part: "a dual-frame payload data input buffer configured for loading one new data block while another data block is being processed in the inner hash engine." Emphasis added.

The Examiner states in the final Office action that col. 45, lines 1 - 10 of Silverbrook teaches this limitation since it teaches the use of temporary registers. Col. 45, lines 2 - 10 state: "Since we only deal with 2 types of messages, our padding can be constant 0s. In addition, the optimized version of the SHA-1 algorithm is used, where only 16 32-bit words are used for temporary storage. These 16 registers are loaded directly by the optimized HMAC-SHA1 hardware. The Nine 32-bit constants h_{1-5} and y_{1-4} are still required, although the fact that

they are constants is an advantage for hardware implementation. Hardware optimized HMAC-SHA-1 requires a total of 1024 bits of data storage:"

The mere use of temporary registers does not imply that such registers are loaded while a data block is being processed. Hence, on its face this passage fails to teach the limitation of the claim. Moreover, col. 4, lines 26 - 45 of Silverbrook illustrate that the registers are loaded separately from other operations. The sixteen registers are shown as X_{N4} where N_4 is incremented from 0 (line 26: "N_4 <- 0") to 15 (line 27: "Do 16 times"). The loading of the registers is designated as "X_{N4} <- InputWord $_{N4}$, etc." in rounds 0 - 4. Here, the loading of X_{N4} is performed after the computations on the right hand side are performed. There is nothing in these operations that teaches or suggests that X_{N4} is loaded while a data block is being processed.

Claim 1 also recites, in part: "an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations." The Examiner states in the final Office action that this limitation is met by col. 45, lines 1 - 10 of Silverbrook (the same passage quoted above).

This passage does not, however, teach or suggest loading hash states for concurrent inner hash and outer hash operations. There is nothing in the passage relating to the recited concurrent operations. Again, on its face this passage fails to teach the limitation of the claim.

Claim 1 also recites, in part: "a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines." The Examiner states in the final Office action that this limitation is met by col. 38 of Silverbrook.

Col. 38 of Silverbrook simply mentions that the system may incorporate a ROM. This passage does not state that such a ROM could be a dual-ported ROM. The term dual-ported ROM appears nowhere in this passage. Moreover, there is no teaching or suggestion that a ROM may advantageously be configured for concurrent constant lookups as claimed.

Applicants thus submit that Claim 1 is not anticipated by or obvious in view of Silverbrook. Claims 2 and 3 that depend on Claim 1 (and the other claims that depend on claim 1) also are patentable over Silverbrook for the reasons set forth above. In addition, these dependent claims are patentable over Silverbrook for the additional limitations that these claims contain.

Claim 16 recites, in part: "pipeline hash operations of said inner hash and outer hash engines, collapse and rearrange multi-round logic to reduce rounds of hash operations, and implement multi-round logic to schedule addition computations to be conducted in parallel with round operations." The Examiner states in the final Office action that this limitation is met by col. 11 and col. 45 of Silverbrook.

Col. 11 merely describes the conventional HMAC algorithm. There is no mention of pipeline operations. Applicant has not found any mention of pipelining anywhere in Silverbrook. Moreover, the cited passages make no mention of any logic to

reduce rounds of hash operations, much less the claimed "collapse and rearrange logic." Finally, the cited passages say nothing about scheduling operations in parallel, much less the specifically recited "addition computations" and "rounds operations."

In view of the above, the Applicants submit that Claim 16 is not anticipated by or obvious in view of Silverbrook. Claims 17 - 22 that depend on Claim 16 (and the other claims that depend on claim 16) also are patentable over Silverbrook for the reasons set forth above. In addition, these dependent claims are patentable over Silverbrook for the additional limitations that these claims contain.

Claim 27 also recites, in part "schedule addition computations to be conducted in parallel with round operations." The Examiner again cites Silverbrook at col. 11, lines 9-27. As argued for Claim 16 above, the passage cited does not disclose the claimed scheduling. Applicant thus submits that Claim 27 and claim 28 that depends on claim 27 are not anticipated by or obvious in view of Silverbrook.

35 U.S.C. §102 Rejections of Claims 14, 29 and 30

Claims 14, 29, and 30 have been rejected under 35 U.S.C. §102(b) as being anticipated by Schneier at pages 442-445. Claims 14 and 29 are independent claims.

Claim 14 recites, in part: "one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative." In the final Office action the Examienr

states that Figure 18.7 shows alternative critical paths. However, Schneier makes no mention of critical paths. Moreover, no alternative paths are described or suggested.

In the final Office action the Examiner states that Schneier teaches steps 4-6 on page 445. However, this portion of Schneier only discusses modifications to MD4 and how they compare to SHA. This section does not say anything regarding alternative paths. Thus, in Schneier the registers are associated with the same path in each successive operation. Accordingly, Schneier does not teach or suggest claim 14 or its dependent claims.

Claim 29 recites, in part: "providing data paths from said five state registers such that four of the five data paths from the registers in any SHA1 round are not timing critical." Schneier does not teach or suggest that any paths are timing critical. It follows then that Schneier does not teach or suggest that it is necessary or desirable to provide data paths that are not timing critical.

In view of the above, the Applicants submit that Claim 29 is not anticipated by or obvious in view of Schneier. Claim 30 that depends on Claim 29 also is patentable over Schneier for the reasons set forth above. In addition, Claim 30 is patentable over Schneier for the additional limitations that Claim 30 contains. For example, as discussed above in conjunction with claim 14 Schneier does not teach or suggest that "in successive SHA1 rounds, registers having the critical path are alternative."

35 U.S.C. §103 Rejections:

The Examiner rejected Claims 4 and 5 and 9 - 12 under 35 U.S.C. §103 as being unpatentable over Silverbrook in view of Sait et al., a scientific article (hereafter "Sait"). Claims 6 and 24 have been rejected under 35 U.S.C. §103 as being patentable over Silverbrook in view of Schneier.

Claims 9-12

Claim 9 in an independent claim. Claims 10 - 12 depend on Claim 9. The Applicants submit that the invention as claimed in Claim 9 is neither taught, described nor suggested by Silverbrook in view of Sait.

Silverbrook and Sait, considered either independently or in combination, do not disclose or suggest Claim 9. Silverbrook does not go into the detail of a hash algorithm and Sait, while not mentioning authentication at all, is about faster multiplications not additions. As explained above, there is no suggestion in either reference or in the art or any motivation to combine these references. Even if the two were combined, their combination would not disclose or suggest Claim 9. For example, the cited references to not disclose or suggest that an addition module may comprise "a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum" as claimed in Claim 9.

Accordingly, the Applicants submit that Claim 9 is not unpatentable over Silverbrook in view of Sait. Claims 10 - 12

that depend on Claim 9 also are patentable over the cited references for the reasons set forth above. In addition, these claims are patentable over the cited references for the additional limitations that these claims contain.

CONCLUSION

In view of the above it is submitted that the claims are patentably distinct over the cited references and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
SDB PAS627920.1-*-07/20/05 5:21 PM